Remarks:

In the Office Action mailed on November 20, 2007 the Examiner rejected claims 1-20. Applicants amend claims 1,3-5, 9, 11 and 14-15 herein. Applicants add new claim 21, for which support can be found in the specification. Accordingly no new subject matter has been added. Claims 1-21 are pending in the application.

The Specification

The Specification was objected to for containing embedded hyperlinks. Applicants have amended the Specification herein to remove such hyperlinks and have filed each hyperlinked reference in an IDS.

The Claims

35 USC 102

Claims 1-20 were rejected under 35 U.S.C. 102(b) as being anticipated by Asunmaa et al. (U.S. Patent Pub. 2003/0172090) (hereinafter "Asunmaa"). Applicants traverse the rejection.

Anticipation under 35 U.S.C. 102(b) requires that each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference. "A claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference", *Verdegaal Bros. v. Union Oil Co. of California*, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987).

A brief summary of Asunmaa and the present patent application may assist in understanding how fundamentally different these two systems are. Applicants describe and claim "a system and method for preventing identity theft during interaction over a computer network"

(page 1, lines. 10-11). The present invention protects a computer user, accessing remote sites over the network from an untrusted computer, from the risks of identity theft (gaining access to the user's personal information without authorization) perpetrated by means such as use of hardware or software keyboard loggers that may exist on the untrusted computer or simply by an intruder looking over a user's shoulder at a video screen monitor found in a public computing location, e.g., an Internet cafe. Applicants' invention involves maintaining personal information on a separate secure computing device (hardware), such as a smart card, that is under the physical control of the user. The invention describes a method whereby the user causes the secure computing device to supply the user's personal information from the secure computing device to various network services through a user interface on the untrusted computer, but where the user never actually enters the user's personal information on the untrusted computer. Thus, keyboard loggers operating on the untrusted computer or simple snooping of activity on the video screen monitors attached thereto cannot be used to gain access to the private information.

Another way to look at the present invention is to consider it as a communications triangle having three nodes: the untrusted computer, the secure computing device, and the remote site accessed over the network. Private information is communicated directly from the secure computing device to the remote site bypassing the untrusted computer. Therefore, the protected private information is never exposed on the untrusted computer and cannot be maliciously obtained on the untrusted computer.

To provide the mechanism by which the server can make the connection between the secure computing device and the untrusted computer, the secure computing device communicates linking information to the remote server. In one embodiment, that linking information

consists of the IP addresses of the secure computing device and of the untrusted client computer.

To ensure that the secure computing device truly is under the control of the user of the untrusted computer, the secure computing device transmits to the server a secret shared between the secure computing device and the user. The server interrogates the user, via the untrusted client computer, to independently determine the user's knowledge of the shared secret. If the user's entered value matches the shared secret transmitted by the secure computing device, the server allows interaction between the server and the user operating on the untrusted client computer.

Asunmaa, on the other hand, relates to a form of providing identities in a manner in which "end-users, devices and other clients [can] easily and simply: identify themselves with an appropriate level of traceability and security; disclose some of their Private Data to various services in a controlled; confidentiality protecting manner so that personal service can be provided; authorize services and other agents to perform certain actions such as sending notifications, charging accounts, etc. All this is done protecting the client's privacy and avoiding needless reveal of the client's real Identity, and with a minimum amount of typing and configuration by the users." (Asunmaa, Paragraph 0071). Asunmaa describe a system which manages "Identities" and discloses a virtual "Identity Card" ("Thus, there is a need for a virtual Identity, which may also be referred to as a personal IdentityCard brand device. With a personal IdentityCard you can confirm who you are." Asunamaa, Paragraph 0067). Asunamaa recognizes the problem of a user to identify themselves to a service. Asunamaa's solution includes providing a virtual Identity Card. The Identity Card acts like a virtual version of a physical identification card ("The IdentityCard allows to securely (sic) use Identities of existing service cards (like bank card, credit card, personal

Identity card, miles card, or any affinity program card) through the personal device or any Internet browser. For instance the bank account may be accessible through both, the physical card and the IdentityCard." Asunamaa, Paragraph 79; "The entire concept for Identities can be seen as a concept for IdentityCards that transfer the use concept and user experience with existing ID cards to electronic devices (PCD and PTD)", Paragraph 104). Asunamaa discusses many aspects of the IdentityCard, e.g., need for or no need for PIN (Paragraph 80), the ability of the Identity Card to replace Username/Password (Paragraph 81), Single Sign On (i.e., the ability to log on once for many services supported by the Identity Card (Paragraph 0083), and so on. However, Asunamaa does not describe a mechanism for allowing a service to securely make the link between a user and an identity.

From these differences, it will be clear that Asunamaa does not teach or suggest Applicants' claimed invention.

Claims 1, 9 and 14

Asunamaa

Claim 1 recites a method of providing secure transactions that involves interactions over a network between three elements, viz., an "untrusted client computer (client)", a "server computer" and a "secure computing device". Accordingly, there are three distinct interactions; namely: an interaction between a client computer and a server, the secure interaction between the secure computing device and the client computer, and the direct interaction between the secure computing device and the server. Furthermore, there is the verification by the server that the communication from the client computer and the secure computing device are indeed to be linked so that the secure computing device may be used by the user to provide information necessary for a user to interact with services provided by the server computer.

Asunamaa does not teach or suggest, at least, the mechanism described and claimed by applicants for providing the complete solution to allow the server to establish an mapping between the user of the untrusted client computer and secure computing device, and independently verifying that the user can establish knowledge of a shared secret known by the secure computing device and communicated to the server.

Claim 1 recites "operating the secure computing device to communicate a list of available services to the client computer." The secure computing device contains stored thereon information useful for interaction with particular services. For example, the user may have stored thereon account information for a particular bank, for a frequent flier program, and for an online merchant. This claimed element is, for example, a recitation of the step of displaying to the user the listing of those services." The Examiner argues that Asunamaa teaches the same at Figure 3, reference number 313 and Paragraph 0174. (Office Action, Page 3, Lines 12-15). However, Applicants respectfully disagree. Paragraph 0174 states:

> "When the user connects to a service (for instance using the browser) or when he clicks a sign-on logo, the *service* first sends the user's client a *list of accepted IdentityCards* or providers of IdentityCards. The user selects an IdentityCard among his IdentityCards, which are also accepted by the service. Given that the service accepts just a specific IdentityCard (for instance for a bank account, for the library, or when you present your personal IdentityCard), the user just chooses to log-on with this card or not. If the user does not have this IdentityCard yet, he might be re-directed to an application form. A new card might also be granted right away for immediate service usage (e.g. by presenting the personal IdentityCard you might be able to open a bank account immediately, and receive the IdentityCard for the bank account)."

Thus, Asunamaa teaches in the cited paragraph that the *service* sends a list of accepted cards. Thus, this is the opposite of the claimed element.

Claim 1 further recites "transmitting from the secure computing device to the server computer user identifying information including a shared secret;

establishing a secure connection from the untrusted client computer to the server computer;

operating the server computer to create a one-to-one mapping between the secure computing device and the untrusted client computer;

receiving an attempted entry of the shared secret by the user from the untrusted client computer;

if the entered shared secret matches the shared secret, permitting the user to interact with a service provided by the server computer."

These elements have been added to Claim 1 (and similarly to the other independent claims). These limitations are directed, for example, to creation of a mapping between the secure computing device and the untrusted computer by the server and the independent verification by the server of the user's knowledge of a shared secret. The mapping is performed to address the need of the server to associate data arriving from the secure computing device on one communications path and data from the untrusted client computer on another communications path. The independent verification of the knowledge of the shared secret is performed by the server to establish that the user has the authority to use the information stored on the secure computing device.

As noted hereinabove, Asunmaa does not teach or suggest a method by which the server performs the steps of creating the linkage between the secure computing device and the untrusted client computer. Furthermore, Asunamaa does not teach or suggest the independent verification of the user's knowledge of a shared secret.

To anticipate a claim, the reference must teach each element of the claim. As discussed hereinabove, Asunmaa fails to teach or suggest several of the elements of Claim 1. Therefore Asunmaa does not anticipate Claim 1 and Claim 1 is patentable over Asunmaa.

Claims 9 and 14 recite analogous limitations to those argued hereinabove in support of Claim 1. Accordingly, Claims 9 and 14 are patentable over Asunmaa for, at least, the same reasons given in support of Claim 1.

35 USC 103

Blatherwick

Claims 16 and 20 stand rejected over the combination of Asunmaa and Blatherwick. Blatherwick like Asunmaa does not teach or suggest:

"transmitting from the secure computing device to the server computer user identifying information including a shared secret;

establishing a secure connection from the untrusted client computer to the server computer;

operating the server computer to create a one-to-one mapping between the secure computing device and the untrusted client computer;

receiving an attempted entry of the shared secret by the user from the untrusted client computer;

if the entered shared secret matches the shared secret, permitting the user to interact with a service provided by the server computer."

Accordingly, Claims 1, 9, and 14 are patentable over Blatherwick also. Since a combination of Asunmaa and Blatherwick would fail to include, at least, these elements, Claims 1, 9, and 14 are patentable over the combination of these two references.

Claims 2-8, 10-13, 15-21.

Claims 2-8, 10-13, 15-21 are all dependant claims deriving from Claims 1, 9, and 14, incorporate the limitation of their respective base claims and provide further unique and non-obvious combinations, and are therefore patentable over Asunmaa and Blatherwick for, at least, the reasons given in support of Claims 1, 9, and 14 and by virtue of such further combinations.

CONCLUSION

It is submitted that all of the claims now in the application are allowable. Applicants respectfully request consideration of the application and claims and its early allowance. If the Examiner believes that the prosecution of the application would be facilitated by a telephonic interview, Applicants invite the Examiner to contact the undersigned at the number given below.

Applicants respectfully request that a timely Notice of Allowance be issued in this application.

Respectfully submitted,

Date: March 20, 2008

/Pehr Jansson/
Pehr Jansson, Reg. No. 35,759

The Jansson Firm
9501 N. Capital of Texas Hwy #202
Austin, TX 78759
512-372-8440
512-597-0639 (Fax)
tony@thejanssonfirm.com